



2131  
#3  
PATENTS  
KWS  
6-11-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

TSUYOSHI TAKAGI

Serial No. 09/654,638

Filed: september 5, 2000

For: **UNDENIABLE DIGITAL SIGNATURE  
BASED ON QUADRATIC FIELD**

)  
)  
)  
) Art Unit: To Be Assigned

)  
) Examiner: To Be Assigned

RECEIVED  
MAR 22 2001  
Technology Center 2100

**INFORMATION DISCLOSURE STATEMENT**

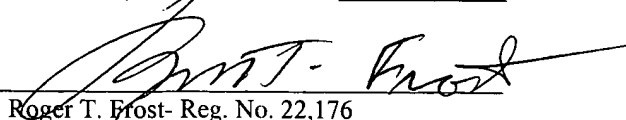
Assistant Commissioner for Patents  
Washington, DC 20231

Sir:

The citation of information on the attached Form PTO/SB/08 is made pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98. A copy of each cited item is enclosed.

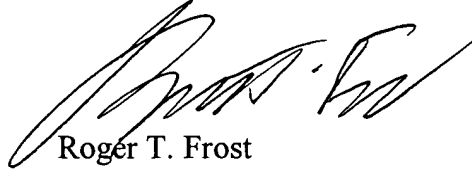
Documents 1-4 were cited in a search report for the European Patent application corresponding to the present application. A copy of the EP Search Report is enclosed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, DC 20231, on March 14, 2001.

  
Roger T. Frost- Reg. No. 22,176

The citation of this information does not constitute an admission of priority or that any cited item is available as a reference, or a waiver of any right the applicant may have under applicable statutes, Rules of Practice in patent cases, or otherwise.

Respectfully submitted,



Roger T. Frost  
Reg. No. 22,176

KILPATRICK STOCKTON LLP  
2400 Monarch Tower  
3424 Peachtree Road, N.E.  
Atlanta, Georgia 30326  
(404) 949-3999  
Our Docket: 13700-0251  
(KS#44471/234055)



Substitute for Form 1449/A/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

**Complete if Known**

|                        |                              |
|------------------------|------------------------------|
| Application Number     | 09/654,638                   |
| Filing Date            | September 5, 2000            |
| First Named Inventor   | Tsuyoshi, Takagi             |
| Group Art Unit         | To Be Assigned               |
| Examiner Name          | To Be Assigned               |
| Attorney Docket Number | 13700-0251 (KS#44471/234055) |

Sheet 1 of 1

**OTHER PRIOR ART - NON PATENT LITERATURE DOCUMENTS**

| Examiner Initials | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published | T <sup>2</sup> |
|-------------------|-----------------------|--|----------------|
|                   | 1                     | HUHNLEIN; <i>A Cryptosystem Based On Non-Maximal Imaginary Quadratic Orders With Fast Decryption</i> ; ADVANCES IN CRYPTOLOGY-EUROCRYPT '98, 1998, PGS 294-307   | ✓              |
|                   | 2                     | MENEZES; <i>Handbook of Applied Cryptography</i> ; 1997, CRC Press, Boca Raton, Florida 33431  | X              |
|                   | 3                     | BUCHMANN; <i>On the Complexity and Efficiency of a New Key Exchange System</i> ; ADVANCES IN CRYPTOLOGY - EUROCRYPT '89; 1990, pgs 597-616   | ✓              |
|                   | 4                     | BIEHL; <i>Cryptographic Protocols Based on Discrete Logarithms in Real-Quadratic Orders</i> ; ADVANCES IN CRYPTOLOGY - CRYPTO '94, 1994, pgs. 56-60  |                |
|                   | 5                     | RIVEST; <i>Obtaining Digital Signatures and Public-Key Cryptosystems</i> ; Communications of the ACM, Feb. 1978, Vol. 21, #2, pgs. 120-126.  |                |
|                   | 6                     | CHAUM; <i>Centre for Mathematics and Computer Science</i> , 1998, Springer-Verlag, pgs. 212-214.   |                |
|                   | 7                     | GENNARO; <i>RSA-Based Undeniable Signatures</i> ; 1998, Springer-Verlag, pgs. 132, 149.  |                |
|                   | 8                     | SHANKS; <i>On Gauss and Composition 1</i> , NUMBER THEORY AND APPLICATIONS, pgs. 163-204, 1989, Kluwer Academic Publishers   | +              |
|                   | 9                     | <i>A Cryptosystem Based on Non-Maximal Imaginary Quadratic Orders with Fast Decryption</i> ; Proceedings Eurocrypt '98; March 1998, pgs. 294-307.  |                |
|                   | 10                    | <i>Conference on the Mathematics of Public Key Cryptography</i> ; June 12, 1999, pgs 1-17  |                |
|                   |                       |  |                |
|                   |                       |  |                |
|                   |                       |  |                |

**RECEIVED**

MAR 22 2001

Technology Center 2100

|                    |  |                 |  |
|--------------------|--|-----------------|--|
| Examiner Signature |  | Date Considered |  |
|--------------------|--|-----------------|--|

<sup>1</sup>Unique citation designation number. <sup>2</sup>Applicant is to place a check mark here if English language translation is attached.